PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-321749
(43)Date of publication of application : 12.12.1997

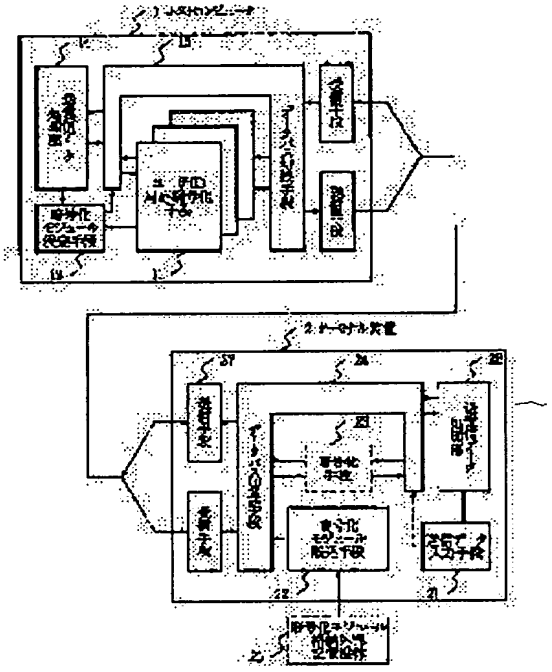
(51)Int.Cl. H04L 9/14
G06F 15/00
G09C 1/00
H04L 9/10

(21)Application number : 08-134823
(22)Date of filing : 29.05.1996

(71)Applicant : CHUBU NIPPON DENKI SOFTWARE KK
(72)Inventor : NANJO MASAYUKI

(54) ON-LINE SECURITY CONTROL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an on-line security control system capable of improving security at an on-line system by enciphering data to transmit/receive between a host computer and a terminal device after log on.
SOLUTION: After checking the propriety of use ID, the host computer 1 selects a user ID corresponding enciphering means 11 corresponding to the user ID to encipher and decode characteristically to the user. In addition, the terminal device 2 reads an enciphering module characteristic to the user to an enciphering means 23 from a portable external storage medium body 25 to encipher and decode characteristically to the user to secure security.



LEGAL STATUS

[Date of request for examination] 29.05.1996
[Date of sending the examiner's decision of rejection] 16.11.1999
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－321749

(43)公開日　平成９年(1997)12月12日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/14			Ｈ０４Ｌ　9/00	６４１	
Ｇ０６Ｆ　15/00	３３０		Ｇ０６Ｆ　15/00	３３０Ａ	
Ｇ０９Ｃ　1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６６０Ｅ	
		7259－5Ｊ		６６０Ａ	
Ｈ０４Ｌ　9/10			Ｈ０４Ｌ　9/00	６２１Ｚ	

審査請求　有　請求項の数３　ＯＬ　（全６頁）

(21)出願番号　特願平8－134823

(22)出願日　平成８年(1996)５月29日

(71)出願人　000213301
中部日本電気ソフトウェア株式会社
愛知県日進市米野木町南山500番地20

(72)発明者　南條　正之
愛知県日進市米野木町南山500番地20　中部日本電気ソフトウェア株式会社内

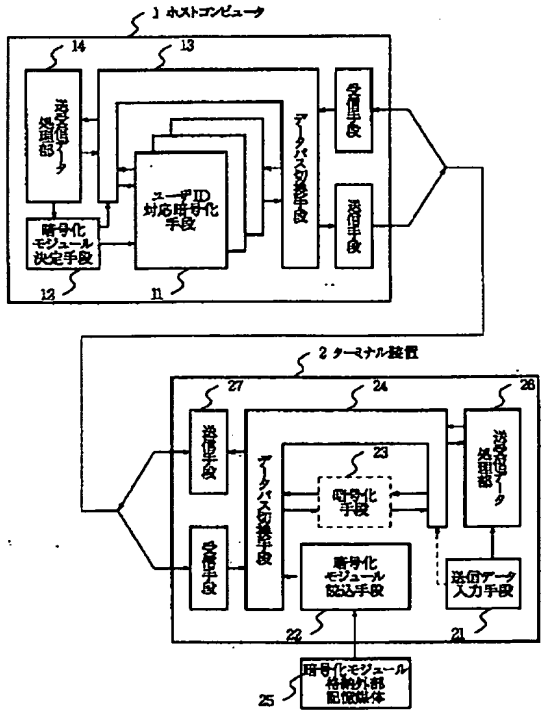
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　オンラインセキュリテイ制御方式

(57)【要約】

【課題】ログオン後は、ホストコンピュータ、ターミナル装置間で送受信するデータを暗号化することにより、オンラインシステムでのセキュリテイを向上できるオンラインセキュリテイ制御方式を提供することにある。

【解決手段】ホストコンピュータ１ではユーザＩＤおよびパスワードの正当性をチェック後ユーザＩＤに応じたユーザＩＤ対応暗号化手段１１を選択してユーザ固有の暗号化および復合化をを行ない、ターミナル装置２では、ユーザ固有の暗号化モジュールを可搬の外部記憶媒体２５から暗号化手段２３に読み出してユーザ固有の暗号化および復号化を行ないセキュリテイを確保する。



1

【特許請求の範囲】

【請求項１】　ターミナル装置側には、送受信データを暗号／復号化する利用者固有の暗号化モジュールを格納する可搬の外部記憶媒体と、前記暗号化モジュールを読み込む暗号化モジュール読込手段と、前記読み込まれた暗号化モジュールにより送信データを暗号化し受信データを復号化する暗号化手段と、送受信データを前記暗号化手段により暗号／復号化するか否かを切り換える第１のデータパス切換手段と、ユーザＩＤやパスワードを含む送信データを入力する送信データ入力手段とを有し、ホストコンピュータ側には、それぞれユーザＩＤに一意に対応して送受信データを暗号／復号化する複数のユーザＩＤ対応暗号化手段と、前記ターミナル装置から送信されたユーザＩＤに応じてこれに対応する前記ユーザＩＤ対応暗号化手段を決定する暗号化決定手段と、通常は前記ユーザＩＤ対応暗号化手段を経由しないパスを形成し前記決定に応じて前記ユーザＩＤ対応暗号化手段を経由するパスを形成する第２のデータパス切換手段とを有することを特徴とするオンラインセキュリテイ制御方式。

【請求項２】　第１のデータパス切換手段は暗号化モジュール読み取りに応じて起動することを特徴とする請求項１記載のオンラインセキュリテイ制御方式。

【請求項３】　第１のデータパス切換手段は送信データ入力手段からの特定の入力に応じて起動することを特徴とする請求項１記載のオンラインセキュリテイ制御方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はオンラインセキュリテイ制御方式に関し、特にログオン後、送受信データをユーザＩＤに対応した暗号化モジュールによって暗号化するオンラインセキュリテイ制御方式に関する。

【０００２】

【従来の技術】従来のオンラインセキュリテイ制御方式は、利用者固有のユーザＩＤおよびパスワードをターミナル装置からホストコンピュータに入力送信し、ホストコンピュータ内で正当性をチェックすることで行なわれていた。

【０００３】また、特開平０４－１６０６６６号公報に示される技術では、予めユーザとその使用装置とを登録しておき、ユーザＩＤおよびパスワードの正当性チェック以外に使用されている装置の正当性をチェックすることで不正な接続を防ぐ方式がとられていた。

【０００４】

【発明が解決しようとする課題】上述した従来のオンラインセキュリテイ制御方式では、ユーザＩＤおよびパスワードは、指紋や装置ＩＤのような人や装置に対して固有なものではなく利用者が記憶しているだけの情報であり、第３者が何らかの手段によってユーザＩＤおよびパスワードを知ることで不正にオンラインシステムに入り込めることができるという問題点を有している。

2

【０００５】また、特開平０４－１６０６６６号公報に見られるような装置ＩＤを正当性をチェックする際の情報に加えた場合、運用上使用できるターミナル装置が限定されるため柔軟性がなく、また、新たに装置を追加する場合や撤去する場合には、ターミナル装置の管理が煩雑になるという欠点がある。

【０００６】本発明の目的は、ログオン後は、ホストコンピュータ、ターミナル装置間で送受信するデータを暗号化し、また、ターミナル装置側ではメモリカードやフレキシブルデイスクのような可搬の外部記憶媒体に格納した暗号化モジュール（プログラム）を使用することにより、オンラインシステムでのセキュリテイを向上させ、運用上のターミナル装置の管理を軽減できるオンラインセキュリテイ制御方式を提供することにある。

【０００７】

【課題を解決するための手段】第１の発明のオンラインセキュリテイ制御方式は、ターミナル装置側には、送受信データを暗号／復号化する利用者固有の暗号化モジュールを格納する可搬の外部記憶媒体と、前記暗号化モジュールを読み込む暗号化モジュール読込手段と、前記読み込まれた暗号化モジュールにより送信データを暗号化し受信データを復号化する暗号化手段と、送受信データを前記暗号化手段により暗号／復号化するか否かを切り換える第１のデータパス切換手段と、ユーザＩＤやパスワードを含む送信データを入力する送信データ入力手段とを有し、ホストコンピュータ側には、それぞれユーザＩＤに一意に対応して送受信データを暗号／復号化する複数のユーザＩＤ対応暗号化手段と、前記ターミナル装置から送信されたユーザＩＤに応じてこれに対応する前記ユーザＩＤ対応暗号化手段を決定する暗号化決定手段と、通常は前記ユーザＩＤ対応暗号化手段を経由しないパスを形成し前記決定に応じて前記ユーザＩＤ対応暗号化手段を経由するパスを形成する第２のデータパス切換手段とを有して構成される。

【０００８】第２の発明のオンラインセキュリテイ制御方式は、第１の発明のオンラインセキュリテイ制御方式において、第１のデータパス切換手段は暗号化モジュール読み取りに応じて起動することを特徴としている。

【０００９】第３の発明のオンラインセキュリテイ制御方式は、第１の発明のオンラインセキュリテイ制御方式において、第１のデータパス切換手段は送信データ入力手段からの特定の入力に応じて起動することを特徴としている。

【００１０】［作用］ターミナル装置から利用者が自分のユーザＩＤおよびパスワードを送信後、ターミナル装置内の暗号化モジュール読込手段が外部記憶媒体中の利用者に固有の暗号化モジュールをターミナル装置内に組み込む。

【００１１】一方、ホストコンピュータでは、ターミナル装置から送信されたユーザＩＤをもとにホストコンピュータ内の暗号化モジュール決定手段がユーザＩＤに対応する暗号化モジュールの中から使用する暗号化モジュールを決定する。

【００１２】これ以降、ホストコンピュータとターミナル装置間で送受信するデータはホストコンピュータ内の暗号化モジュールとターミナル装置内の暗号化モジュールによって暗号化される。

【００１３】このため、利用者固有のターミナル装置側の暗号化モジュールを持たない不正な利用者は、意図する不正行為を実行できない。

【００１４】また、ターミナル装置が変わっても暗号化モジュールが格納された外部記憶媒体をセットすることによりターミナル装置の管理情報を変更することなく利用できる。

【００１５】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００１６】図は本発明のオンラインセキュリティ制御方式の一実施の形態を示すブロック図である。

【００１７】本実施の形態のオンラインセキュリティ制御方式は、図１に示すように、ターミナル装置２内に、送受信データを暗号／復号化する利用者固有の暗号化モジュールを格納する暗号化モジュール格納外部記憶媒体２５と、この暗号化モジュール格納外部記憶媒体２５から暗号化モジュールを暗号化手段２３内のメモリに読み込む暗号化モジュール読込手段２２と、ホストコンピュータ１へ送信するユーザＩＤやパスワードデータを利用者に入力させる送信データ入力手段２１と、送受信データを暗号化モジュールにより暗号化する暗号化手段２３と、暗号化手段２３によって暗号／復号化するか否かを切り換えるデータパス切換手段２４とを有している。

【００１８】一方、ホストコンピュータ１内には、ユーザＩＤに一意に対応し送受信データを暗号／復号化するユーザＩＤ対応暗号化手段１１と、ターミナル装置２から送信されたユーザＩＤにより対応するユーザＩＤ対応暗号化手段１１を決定する暗号化モジュール決定手段１２と、ユーザＩＤ対応暗号化手段１１を決定後送信データをユーザＩＤ対応暗号化手段１１によって暗号／復号化する処理に切り換えるデータパス切換手段１３とを有している。

【００１９】暗号化モジュール格納外部記憶媒体２５はフレキシブルディスクやメモリカード等可搬性が高いものが望ましい。

【００２０】暗号化モジュール格納外部記憶媒体２５に格納されている暗号化モジュールはコード変換テーブルにより送受信データを暗号／復号化するものや計算により暗号／復号化するもの等がある。

【００２１】データパス切換手段２４は送信データ入力

手段２１がユーザＩＤやパスワードデータ送信して後に暗号化モジュールを読み取りその後、自動的に切り換える方式と利用者がキーボード操作により任意の時点で切り換える方式等がある。

【００２２】次に、本実施の形態のオンラインセキュリティ制御方式の動作について、図１を参照して詳細に説明する。

【００２３】オンライン処理を開始する場合、ターミナル装置２内の送信データ入力手段２１を使用して利用者は自分のユーザＩＤおよびパスワードを入力する。

【００２４】入力されたデータは、受信データの画面表示やキーボード入力データ、ファイルデータの送信データ編集等の従来のデータ処理を行なう送受信データ処理部２６を経由しデータパス切換手段２４に供給される。

【００２５】オンライン処理開始時は暗号化を行なわないパスを規定値として暗号化手段２３を経由せずそのまま送信手段２７からホストコンピュータ１に送信される。

【００２６】ターミナル装置２からのユーザＩＤおよびパスワードデータをホストコンピュータ１が受信すると、ユーザＩＤおよびパスワードデータはデータパス切換手段１３に供給され暗号化を行なわないパスを規定値としてユーザＩＤ対応暗号化手段１１を経由せずそのまま送受信データ処理部１４に供給される。

【００２７】送受信データ処理部１４でユーザＩＤおよびパスワードの正当性をチェックし、正しければ暗号化モジュール決定手段１２によってユーザＩＤに対応するユーザＩＤ対応暗号化手段１１を決定し、データパス切換手段１３によって暗号化を行なうパスに切り換える。

【００２８】一方、ターミナル装置２において、ユーザＩＤおよびパスワードが正当とホストコンピュータ１に判断されたことを認知できた時点で暗号化モジュール読込手段２２を使用して暗号化モジュール格納外部記憶媒体２５の暗号化モジュールを暗号化手段２３内に読み込み、その後、データパス切換手段２４は暗号化を行なうパスに切り換える。

【００２９】これ以降、ホストコンピュータ１とターミナル装置２との間で送受信されるデータは、ホストコンピュータ１内のユーザＩＤ対応暗号化手段１１によって、また、ターミナル装置２内の暗号化手段２３によって暗号／復号化される。

【００３０】次に、本発明の実施例について図面を参照して説明する。

【００３１】図２を参照すると、本発明の実施例のオンラインセキュリティ制御方式のターミナル装置３０はパソコン通信を行なうターミナル装置３０であり、モデム４０経由で公衆回線に接続する。

【００３２】図１と図２とを対比すると、暗号化モジュールを格納する暗号化モジュール格納外部記憶媒体２５は暗号化モジュール格納フレキシブルディスク３５であ

り、暗号化モジュール読込手段２２はフレキシブルデイスク装置３２であり、送信データ入力手段２１はキーボード３１としてある。

【００３３】暗号化モジュールは、図３（ｃ）に示す受信データ変換テーブル２３－Ｒと図３（ｄ）に示す送信データ変換テーブル２３－Ｓとを持ち、受信データおよび送信データをテーブル引きにて変換する方式である。

【００３４】暗号／復号化するか否かの切り換えは利用者のキーボード３１からの指示によってデータパス切換手段２４が行なう。

【００３５】ホストコンピュータ１側はターミナル装置３０から正しいパスワードを受信した時点で暗号化モジュールを経由するパスに切り換えるものとする。

【００３６】次に、本発明の実施例の動作について、図２、３および４の参照して詳細に説明する。

【００３７】図２を参照すると、ターミナル装置３０側の暗号化手段２３を制御する暗号化モジュールは暗号化モジュール格納フレキシブルデイスク３５に格納されており、降順のアルファベットのそれぞれの文字を昇順のアルファベットのそれぞれの文字に順に対応して変換する受信データ変換テーブル２３－Ｒと送信データ変換テーブル２３－Ｓとを持ち、図３（ａ）および（ｂ）の流れ図に示すように、送受信データをこれらのテーブル引きにより変換する暗号化方式をとる。

【００３８】パソコン通信を開始すると、受信データを画面に表示したりキーボード３１からの入力データを送信する従来の通信処理を行なう送受信データ処理部２６がキーボード入力送信データや受信データ表示を行なう。このとき、ターミナル装置３０内のデータパスは暗号化を行なわないパスとなっており送受信データは暗号化手段２３を経由することはない。

【００３９】先ず、暗号化しない通常の場合について説明する。

【００４０】パソコン通信では通常図４（ａ）に示すように、ユーザＩＤおよびパスワードをターミナル装置３０からモデム４０経由でホストコンピュータ１に送信し（図４（ａ）ａ－１）、ホストコンピュータ１側で正当性をチェックし正しければ処理を続行できる仕組みとなっている。

【００４１】よって、利用者にとってはユーザＩＤおよびパスワード入力後次に続くべきメッセージを受信することで（図４（ａ）ａ－２）、ユーザＩＤおよびパスワードがホストコンピュータ１側で確認されたことを判断でき、以後、継続して通信を行なうことができる。これが従来の方式である。

【００４２】次に先ず、ホストコンピュータ１が暗号化対応した場合についての動作を説明する。

【００４３】パスワード入力送信後（図４（ｂ）ｂ－１）、ホストコンピュータ１は次に続くべきメッセージを暗号化してターミナル装置３０に送信し（図４（ｂ）ｂ－２）、ターミナル装置３０からの入力送信待ちとなる。

【００４４】暗号化モジュールを持たない不正な利用者が接続を試みた場合は、受信したデータは暗号化されたデータである図４（ｂ）ｂ－２の「プロフアイルヲシュウセイシマスカ（Ｂ，Ｍ，ＴＤ）＝」までのデータ表示となって、対応する暗号化モジュール格納フレキシブルデイスク３５を持っていないので、復号化することができず、その後の意図する不正行為を行なうことができない。

【００４５】しかし、正常利用者の場合には、暗号化モジュール格納フレキシブルデイスク３５をフレキシブルデイスク装置３２にセットしキーボード３１の操作によりデータパス切換手段２４にデータパス切り換えを要求する。

【００４６】データパス切換手段２４はフレキシブルデイスク装置３２にセットされた暗号化モジュール格納フレキシブルデイスク３５内の暗号化モジュールを暗号化手段２３内に読み込み、ターミナル装置３０のデータパスを暗号化を行なうパスに切り換え暗号化対応を行なう。

【００４７】このデータパス切り換えによってターミナル装置３０はホストコンピュータ１から送られてくる暗号化された受信データを暗号化手段２３によって復号化し、送受信データ処理部２６で、例えばキーボード３１よりの２度の「Ｎ」入力を経て、図４（ｂ）ｂ－２の「お知らせを表示しますか（Ｙ，Ｎ）＝Ｎ」までのように表示し、正常利用者は相続いて次のキーボード入力送信を暗号化手段２３によって暗号化して送信することとなる。

【００４８】以上説明したように、本実施の形態および実施例のオンラインセキュリテイ制御方式は、ログオン後、ホストコンピュータとターミナル装置の間で送受信するデータをユーザＩＤに対応した方式で暗号化するため、暗号化モジュールを持たない不正な利用者が意図する不正行為を行なうことができず、これにより機密情報の入手やデータの改竄、破壊等の不正な利用者の悪意による行為を防ぐことができる。

【００４９】また、可搬性のある外部記憶媒体に利用者固有の暗号化モジュールを格納するので、装置ＩＤを使用している特開平０４－１６０６６６号公報記載の技術のように利用できるターミナル装置に限定されず任意のターミナル装置でオンライン処理を行なうことができ、これによりターミナル装置を追加または撤去する場合、ターミナル装置の管理情報等を変更する必要はなく、管理の簡単化ができる。

【００５０】

【発明の効果】以上説明したように、本発明のオンラインセキュリテイ制御方式は、ログオン後、ホストコンピュータとターミナル装置の間で送受信するデータをユー

ザＩＤに対応した方式で暗号化するため、暗号化モジュールを持たない不正な利用者が意図する不正行為を行なうことができず、これにより機密情報の入手やデータの改竄、破壊等の不正な利用者の悪意による行為を防ぐことができるという効果を有する。

【００５１】また、可搬性のある外部記憶媒体に利用者固有の暗号化モジュールを格納するので、装置ＩＤを使用している特開平０４－１６０６６６号公報記載の技術のように利用できるターミナル装置に限定されず任意のターミナル装置でオンライン処理を行なうことができ、これによりターミナル装置を追加または撤去する場合、ターミナル装置の管理情報等を変更する必要はなく、管理の簡単化ができるという効果を有している。

【図面の簡単な説明】

【図１】本発明のオンラインセキュリテイ制御方式の一実施の形態を示すブロック図である。

【図２】本発明のオンラインセキュリテイ制御方式の一実施例のターミナル装置の構成を示すブロック図である。

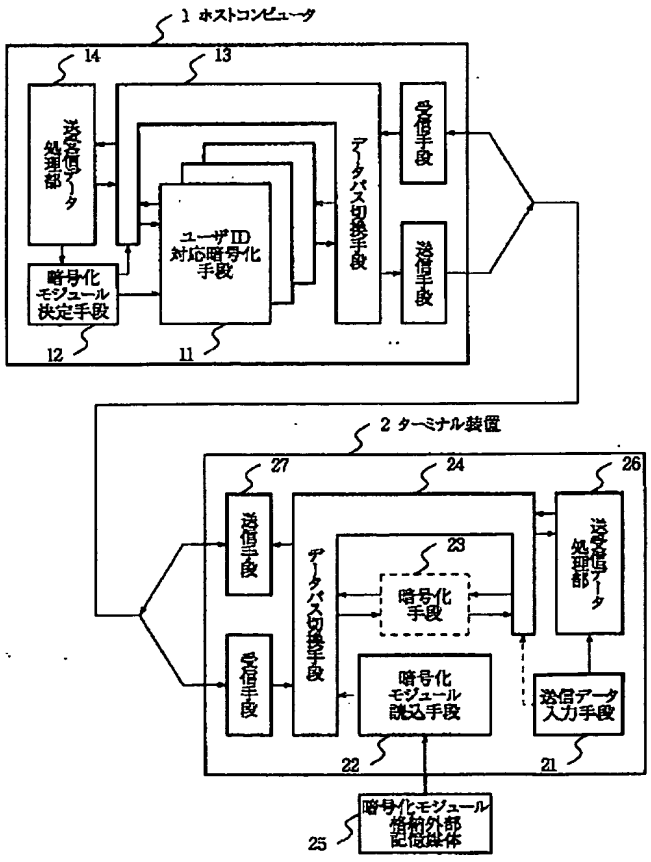
【図３】（ａ）は本発明のオンラインセキュリテイ制御方式の一実施例のデータ受信時の動作を示す流れ図、（ｂ）はデータ送信時の動作を示す流れ図、（ｃ）は受信データ変換テーブルを示すテーブル図、（ｄ）は送信データ変換テーブルを示すテーブル図である。

【図４】（ａ）は従来の暗号化しないときのターミナル装置に表示されるメッセージ表示図、（ｂ）は暗号化対応した場合のターミナル装置に表示されるメッセージ表示図である。

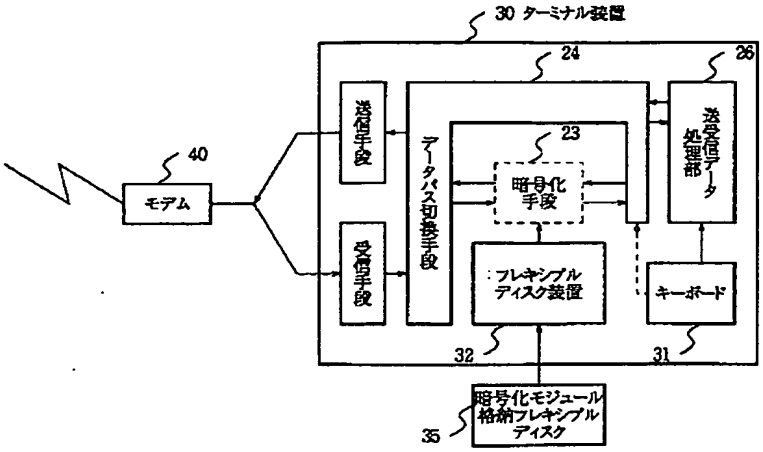
【符号の説明】

１　ホストコンピュータ
２、３０　ターミナル装置
１１　ユーザＩＤ対応暗号化手段
１２　暗号化モジュール決定手段
１３、２４　データバス切換手段
１４、２６　送受信データ処理部
２１　送信データ入力手段
２２　暗号化モジュール読込手段
２３　暗号化手段
２５　暗号化モジュール格納外部記憶媒体
２７　送信手段
３１　キーボード
３２　フレキシブルデイスク装置
３５　暗号化モジュール格納フレキシブルデイスク
４０　モデム

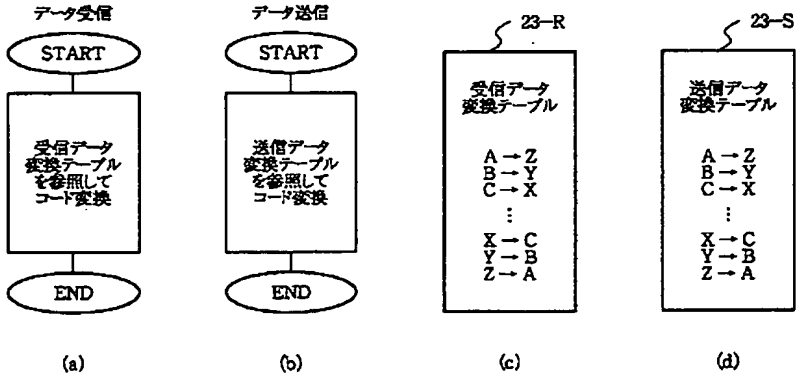
【図１】



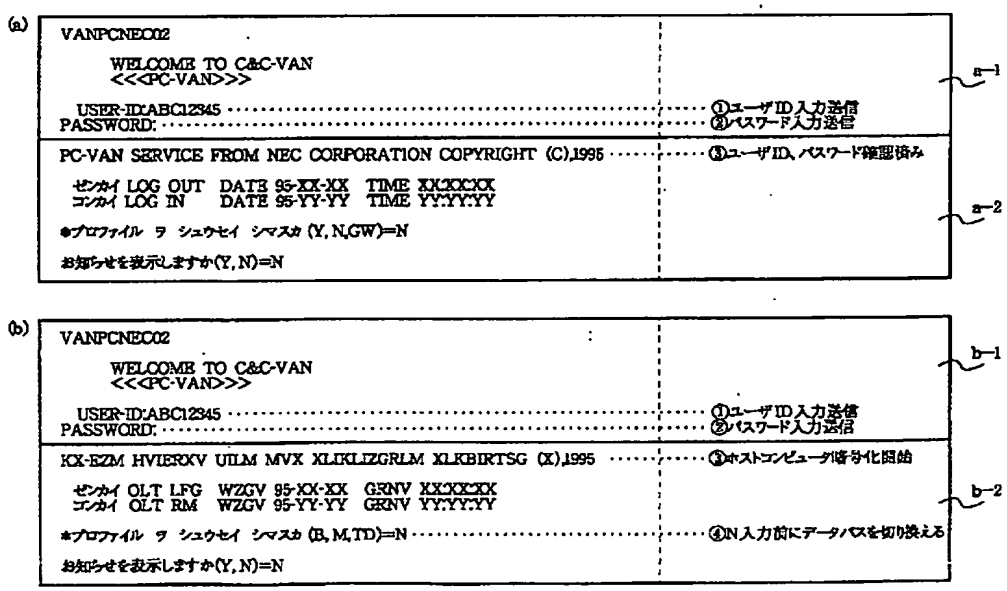
【図２】


30 ターミナル装置
24
26
23
40
モデム
送信手段
受信手段
データパス切換手段
暗号化手段
フレキシブルディスク装置
キーボード
送受信データ処理部
32
31
暗号化モジュール格納フレキシブルディスク
35

【図３】


データ受信
START
受信データ変換テーブルを参照してコード変換
END
(a)
データ送信
START
送信データ変換テーブルを参照してコード変換
END
(b)
23-R
受信データ変換テーブル
A → Z
B → Y
C → X
X → C
Y → B
Z → A
(c)
23-S
送信データ変換テーブル
A → Z
B → Y
C → X
X → C
Y → B
Z → A
(d)

【図４】


(a)
VANPCNEC02
WELCOME TO C&C-VAN
<<<PC-VAN>>>
USER-ID:ABC12345
PASSWORD:
①ユーザID入力送信
②パスワード入力送信
a-1
PC-VAN SERVICE FROM NEC CORPORATION COPYRIGHT (C),1995
③ユーザID、パスワード確認済み
センカイ LOG OUT DATE 95-XX-XX TIME XX:XX:XX
コンカイ LOG IN DATE 95-YY-YY TIME YY:YY:YY
*プロファイル ヲ シュウセイ シマスカ (Y,N,GW)=N
お知らせを表示しますか(Y,N)=N
a-2
(b)
VANPCNEC02
WELCOME TO C&C-VAN
<<<PC-VAN>>>
USER-ID:ABC12345
PASSWORD:
①ユーザID入力送信
②パスワード入力送信
b-1
KX-EZM HVIERXV UILM MVX XLIKLIZGRLM XLKBIRTSG (X),1995
③ホストコンピュータ暗号化開始
センカイ OLT LFG WZGV 95-XX-XX GRNV XX:XX:XX
コンカイ OLT RM WZGV 95-YY-YY GRNV YY:YY:YY
*プロファイル ヲ シュウセイ シマスカ (B,M,TD)=N
④N入力前にデータパスを切り換える
お知らせを表示しますか(Y,N)=N
b-2